REMARKS

Claims 1-6 and 13-30 were pending. Claims 1, 6, 13-17, 19-20, 23-24, and 28 have been amended. Claim 18 have been cancelled. Claims 31 is newly submitted. No new matter has been added. Accordingly, claims 1-6, 13-17, and 19-31 remain pending in the application. Reconsideration is respectfully requested in view of the amendments to the claims and the following remarks.

I. The § 102/103 Rejections

Claims 1-3, 17, 19, 21, 23, and 25 stand rejected under 35 U.S.C. § 102(a) as being anticipated by U.S. Patent No. 6,401,183 ("Rafizadeh").

Claims 4-6, 13-16, 18, 20, 24, and 28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Rafizadeh in view of U.S. Patent No. 6,542,979 ("Eckardt").

Claims 26-27 and 29-30 rejected under 35 U.S.C. § 103(a) as being unpatentable over Rafizadeh, in view of U.S. Patent Publication No. 2003/0163610 ("Stevens") and E.P. van Westendorp "Hidden Partitions" ("Westendorp").

Claims 1-3, 17, 19, 21, 23, and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Westendorp in view of "Information Technology - AT Attachment with Packet Interface – 6 (ATA/ATAPI-6)", working draft T13 1410D Revision 3a, 14 December 2001, pages 44-45 ("McLean").

Claims 4-6, 13-16, 18, 20, 24, and 28 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Westendorp, in view of McLean and Eckardt.

Claims 26, 27, and 29-30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Westendorp, in view of McLean and Stevens.

Applicant respectfully traverses the rejections.

Claim 1, as amended, recites detecting a special boot condition during a pre-boot test of the computer system, in which the special boot condition is a hardware tamper detect or a software tamper detect. In response to detecting the special boot condition, a size of a partition of the hardfile is adjusted to alter an operating system access configuration of the hardfile. The size of the partition of the hardfile is adjusted to reduce access of the operating system to data stored on the hardfile during the hardware tamper or the software tamper.

A. *Rafizadeh Fails To Disclose Adjusting a Size of a Partition of a Hardfile To Alter an Operating System Access Configuration of the Hardfile in Response To Detection of a Hardware Tamper or a Software Tamper During a Pre-Boot Test of a Computer System*

Rafizadeh discloses a Storage Manager that enables the dynamic partitioning and manipulation of partitions within a secondary storage of a computer device (see Abstract; col. 3, ll. 63-67). In particular, the Storage Manager takes control of a computer device before a run-time operating system is enabled on the computer device. To this end, Rafizadeh discloses changing the format of a master boot record (MBR) to include a 12 byte Storage Manager Pointer Field 22 (see FIG. 3), which contains the starting logical block address of the executable code for the Storage Manager (col. 4. l. 65 – col. 5, l. 11). Alternatively, Rafizadeh discloses that the Storage Manager can be executed at the proper time by embedding the Storage Manager executable code within FLASH BIOS memory (col. 5, ll. 12-18).

While Rafizadeh discloses using a Storage Manager to dynamically adjust partitions within a secondary storage of a computer device, Rafizadeh nevertheless fails to disclose adjusting a size of a partition of the hardfile to alter an operating system access configuration of the hardfile in response to detection of a hardware tamper or a software tamper, as required by

claim 1. Instead, as discussed above, Rafizadeh discloses that the Storage Manager is activated based on a Storage Manager Pointer Field 22 within a master boot record, or based on Storage Manager executable code within a FLASH BIOS memory. Merely, executing code that exists does not correspond to detection of a software tamper or a hardware tamper. For example, claim 6 recites that a hardware tamper corresponds to installation of new hardware for use with the computer system and that a software tamper corresponds to installation of a new software application on the computer system.

In rejecting claim 6, the Examiner states that "Rafizadeh discloses the boot condition is user's modification". Applicant respectfully disagrees. As discussed above, the Store Manager is activated based on a Storage Manager Pointer Field 22 within a master boot record, or based on Storage Manager executable code within a FLASH BIOS memory. There is no detection of a user modification involved in activating the Storage Manager other than to execute a master boot record. Thus, though hardware and software can be logically equivalent, activatation of a Store Manager based on a Storage Manager Pointer Field within a master boot record, or based on Storage Manager executable code within a FLASH BIOS memory does not suggest using a detect of a software tamper or a hardware tamper as a boot condition.

B. *Westendorp Fails To Disclose Adjusting a Size of a Partition of a Hardfile To Alter an Operating System Access Configuration of the Hardfile in Response To Detection of a Hardware Tamper or a Software Tamper During a Pre-Boot Test of a Computer System*

Westendorp is an online thread discussion regarding a question of how to find a hidden partition within a computer system. Westendorp discloses use of a "SET MAX ADDRESS" command that is normally issued by a system BIOS to create a reserved area for data storage that

is outside of the normal operating system file system. Such a teaching is consistent with Applicant's specification at page 6, lines 2-10. Westendorp suggests that a program may temporarily set the max address at the max native address, perform a write or read, and then restore the original max address. However, as acknowledged by the Examiner, Westendorp fails to disclose when the SET MAX ADDRESS command. Consequently, Westendorp fails to disclose adjusting a size of a partition of the hardfile to alter an operating system access configuration of the hardfile in response to detection of a hardware tamper or a software tamper, as required by claim 1.

In rejecting claim 6, the Examiner states that "Westendorp discloses that the boot condition is whether to execute SET MAX ADDRESS command to access a hidden partition". The Examiner further acknowledges that Westendorp fails to disclose a boot condition being a hardware tamper detect. However, the Examiner asserts that because hardware and software are logically equivalent, it would have been obvious to use a hardware tamper detect as the boot condition. Applicant respectfully disagrees. Though hardware and software can be logically equivalent, even assuming *arguendo* that Westendorp discloses a boot condition to be whether to execute SET MAX ADDRESS command to access a hidden partition, such action does not teach or suggest using a detect of a software tamper or a hardware tamper as a boot condition.

C. *McLean Fails To Disclose Adjusting a Size of a Partition of a Hardfile To Alter an Operating System Access Configuration of the Hardfile in Response To Detection of a Hardware Tamper or a Software Tamper During a Pre-Boot Test of a Computer System*

As acknowledged by the Examiner, McLean discloses that the SET MAX ADDRESS command is intended for use only by system BIOS or other low-level boot time process.

Nevertheless, McLean fails to disclose adjusting a size of a partition of the hardfile to alter an operating system access configuration of the hardfile in response to detection of a hardware tamper or a software tamper. Instead, McLean discloses only that the SET MAX ADDRESS command is used on system reset or on a save to a disk, and McLean fails to disclose that a system reset or a save to a disk includes a detection of a hardware tamper or a software tamper.

D. *Eckardt Fails To Disclose Adjusting a Size of a Partition of a Hardfile To Alter an Operating System Access Configuration of the Hardfile in Response To Detection of a Hardware Tamper or a Software Tamper During a Pre-Boot Test of a Computer System*

Eckardt discloses a supplemental driver that is stored outside of the master boot record of a disk drive, which supplemental driver is used to access a hidden disk partition (see Abstract). In particular, Eckardt discloses that if a "hot key" is pressed during boot of the disk drive, then the supplemental driver is combined with a driver from the master boot record which permits an operating system to access both legal partitions and illegal partitions. If the "hot key" is not pressed, then the operating system only has access to the legal partitions of the hard drive (col. 1, line 61 – col. 2, line 13).

While Eckardt discloses granting an operating system access to a more (or less) partitions of a hard drive to control operating system access to data on the hard drive, Eckardt clearly fails to disclose adjusting a size of a partition of the hardfile to alter an operating system access configuration of the hardfile in response to detection of a hardware tamper or a software tamper. Instead, as discussed above, Eckardt discloses only changing the number of partitions that an operating system can access during boot up depending upon whether a "hot key" is pressed. As discussed above, a hardware tamper can correspond to installation of new hardware for use with

the computer system and a software tamper can correspond to installation of a new software application on the computer system. The pressing of a "hot key" does not is not equivalent to either of these cases.

E. *Stevens Fails To Disclose Adjusting a Size of a Partition of a Hardfile To Alter an Operating System Access Configuration of the Hardfile in Response To Detection of a Hardware Tamper or a Software Tamper During a Pre-Boot Test of a Computer System*

Stevens discloses a computer system and method for emulating a non-volatile removable media device (e.g., a CD-ROM or DVD drive) by storing material from non-volatile removable media onto a mass storage device (e.g., a hard drive) (see Abstract). Specifically, the material from a CD or DVD is stored in a PARTIES service area of the hard drive, and an operating system of the computer system accesses the stored in the PARTIES service area during emulation of a CD-ROM or DVD drive (see paragraphs [0019]-[0020]). The operating system is configured to access the PARTIES service area through use of a boot engineering extension record (BEER) that, in turn, is configured to have a SETMAX pointer that points to a user area of the hard drive and a service area pointer that points to a PARTIES service area (paragraph [0024].

Stevens, however, fails to disclose adjusting a size of a partition of the hardfile to alter an operating system access configuration of the hardfile in response to detection of a hardware tamper or a software tamper. The transfer of data from a CD or DVD to hard drive is not equivalent to a hardware tamper or a software tamper. For example, as discussed above, a hardware tamper can correspond to installation of new hardware for use with the computer system

and a software tamper can correspond to installation of a new software application on the computer system (see claim 6).

Moreover, in response to transferring data to a hard drive, Steven discloses granting an operating system greater access to partitions of the hard drive (i.e., the user area 34 in addition to the PARTIES service area 35a) (see paragraph [0025]; FIG. 2). In contrast, claim 1 recites the size of the partition of the hardfile is adjusted to reduce access of the operating system to data stored on the hardfile during the hardware tamper or the software tamper. Thus, Stevens teaches away from elements recited in claim 1.

F. *The claim has limitations not taught by the references*

To support a finding of anticipation under 35 U.S.C. §102 a single piece of prior art must disclose each and every limitation of the claimed invention.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art.

Neither Rafizadeh, Westendorp, McLean, Eckardt, nor Stevens discloses adjusting a size of a partition of the hardfile to alter an operating system access configuration of the hardfile in response to detection of a hardware tamper or a software tamper. Consequently, neither Rafizadeh, Westendorp, McLean, Eckardt, nor Stevens (either alone or in combination) can anticipate or render claim 1 obvious.

G. *Other Independent Claims*

Independent claims 13-17, 19, 23 and 28 (and the claims that depend therefrom) each incorporates limitations similar to claim 1, and are also allowable over the references cited above for reasons corresponding to those set forth in connection with claim 1.

Applicant submits that 1-6, 13-17, and 19-31 are allowable over the references cited above and are in condition for allowance. Should any unresolved issues remain, the Examiner is invited to call the undersigned at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

March 5, 2007

Kelvin M. Vivian
Attorney for Applicant(s)
Reg. No. 53,727
(650) 475-1448